PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : G06K 19/073, B42D 15/10 // 109:00, 201:00 — A1

(11) International Publication Number: WO 98/01820

(43) International Publication Date: 15 January 1998 (15.01.98)

(21) International Application Number: PCT/AU97/00426

(22) International Filing Date: 3 July 1997 (03.07.97)

(30) Priority Data:
P00848 5 July 1996 (05.07.96) AU

(71) Applicant (*for all designated States except US*): DYNAMIC DATA SYSTEMS PTY. LTD. [AU/AU]; 7th floor, 227 Collins Street, Melbourne, VIC 3000 (AU).

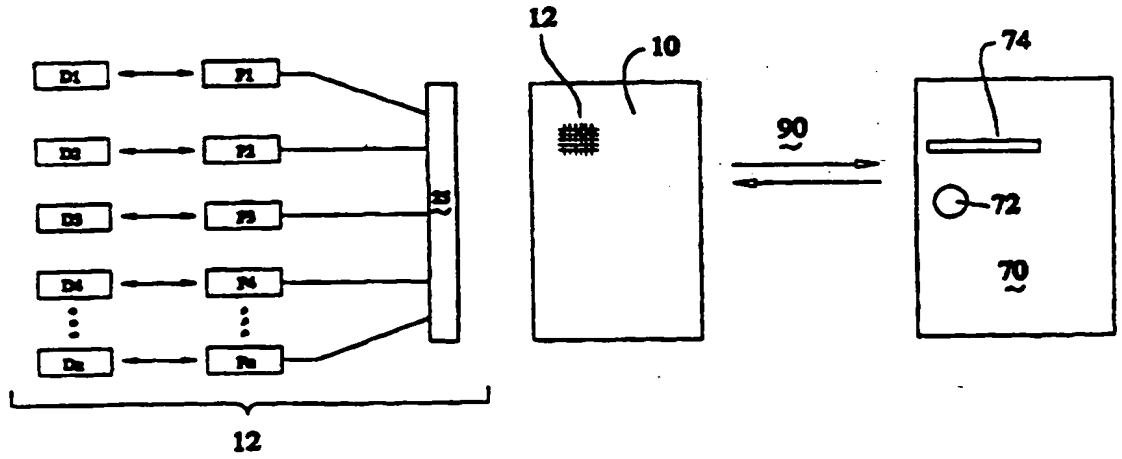
(72) Inventor; and
(75) Inventor/Applicant (*for US only*): ELBAUM, Hector, Daniel [AU/AU]; 11 Harrington Place, Doncaster East, VIC 3109 (AU).

(74) Agent: WILSON, Stephen, Henry; Griffith Hack, 509 St Kilda Road, Melbourne, VIC 3004 (AU).

(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, HU, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW, ARIPO patent (GH, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).

Published
With international search report.

(54) Title: IDENTIFICATION STORAGE MEDIUM AND SYSTEM AND METHOD FOR PROVIDING ACCESS TO AUTHORISED USERS



(57) Abstract

An identification storage medium such as a card (10) is disclosed. The card (10) contains data relating to a user such as cred card information, EFTPOS information, licence information or the like. The card (10) includes and integrated circuit (12) which contai biometric data relating to the user and which can be read from the card by a reader (20, 70). The reader also includes a scanner for scannir the biometric data such as a thumbprint of the user so that the scan data can be compared with the data read from the card to establish th user's authenticity. The comparison can take place in the circuit (12) or in the reader. The integrate circuit (12) preferably also includ a plurality of separate data storage locations D1 to Dn for storing separate data parcels and includes separate programs P1 to Pn each f accessing one of the storage locations D1 to Dn. Upon receipt of an appropriate authorisation code, one or more of the programs P1 to P is activated to access only data in the corresponding storage location D1 to Dn so that only that data is read from the card.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece	ML	Mali	TR	Turkey
BG	Bulgaria	HU	Hungary	MN	Mongolia	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MR	Mauritania	UA	Ukraine
BR	Brazil	IL	Israel	MW	Malawi	UG	Uganda
BY	Belarus	IS	Iceland	MX	Mexico	US	United States of America
CA	Canada	IT	Italy	NE	Niger	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NL	Netherlands	VN	Viet Nam
CG	Congo	KE	Kenya	NO	Norway	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NZ	New Zealand	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	PL	Poland		
CM	Cameroon	KR	Republic of Korea	PT	Portugal		
CN	China	KZ	Kazakstan	RO	Romania		
CU	Cuba	LC	Saint Lucia	RU	Russian Federation		
CZ	Czech Republic	LI	Liechtenstein	SD	Sudan		
DE	Germany	LK	Sri Lanka	SE	Sweden		
DK	Denmark	LR	Liberia	SG	Singapore		
EE	Estonia						

IDENTIFICATION STORAGE MEDIUM AND SYSTEM AND METHOD FOR PROVIDING ACCESS TO AUTHORISED USERS

This invention relates to an identification storage medium and to a system and method for providing access to authorised users.

EFTPOS (Electronic Funds Transfer Point) terminals have operated for many years whereby a card is swiped through the device so a card reader can read data on the card to obtain account details. Usually an account type and a personal identification number are entered by the user and the information is transmitted to a facility, usually a bank or other finance establishment, for electronic authorisation. The information is processed through a pin pad which encrypts the personal identification number details for data security. The data is sent via a modem through specialised phone lines to a transactions switching network, where it is switched through the correct banks, host computers to obtain bank authorisation. Once authorisation is provided a financial transaction is allowed to proceed whereby a user may purchase goods or obtain cash.

Cards including encrypted data are also used for providing access to secure premises or secure areas as well as for conducting financial transactions. In order to provide access to a secured area a user may swipe the card through a card reader and enter a pin number which, if a match is obtained with information read from the card, grants access to the secure area.

As the worldwide use of financial transaction cards such as credit/debit cards has increased the incidence of card fraud has also increased. This fraud results in a multi-

million dollar loss to both the banks and the credit companies, which in turn is passed on to users in the form of charges. To combat this fraud, card manufacturers have utilised a number of different methods to assure security, including tamper-proof signature strips, holograms, personal identification numbers (as discussed above) and photo identification. Unfortunately, all of these methods have only managed to provide a brief respite and have had no significant effect on the operations of the organised counterfeiting rings.

The object of this invention is to provide a storage medium and system and method for providing access which are cost effective and which also provide the required security.

The reference to the provision of access in this specification should be understood to mean access to a financial transaction by way of transfer of funds to purchase goods or receipt of cash, personal identification such as date of birth, licence details etc, or physical access to secured premises or areas.

The invention may be said to reside in an identification storage medium, including:

a support member; and

circuit means supported by the support member for storing biometric data relating to an authorised user of the medium.

Preferably the biometric data is a fingerprint template of the user. However, in other embodiments the biometric data may comprise other biological information such as DNA information and/or iris information or the like which may be stored and compared.

Preferably the storage medium comprises a plastic card similar in size and shape to a credit card.

Preferably the circuit means comprises an integrated circuit chip supported by the body of the credit card.

The invention may also be said to reside in an identification system for providing access to an authorised user, including:

a storage medium having a support member, and

circuit means supported by the support member for storing biometric data relating to the authorised user;

a sensor for access by a user to provide biometric data to the system; and

processing means for comparing the biometric data stored in the circuit means with that detected by the sensor and for providing an access signal in the case of a match to thereby grant access to the authorised user.

The invention may also be said to reside in an identification method for providing access to an authorised user, including:

storing biometric data relating to an authorised user on a storage medium;

comparing the biometric data stored on the storage medium with biometric data provided by a user; and

granting access to the authorised user in the case of a match between the data stored on the storage medium and that provided by the user.

In preferred embodiments of the invention the storage medium comprises a financial transaction identification card and the card may include additional data relating to account details. The additional data may be included in the circuit means which contains the biometric data or may

be included on a magnetic strip or the like separate from the circuit means which contains the biometric data.

After access has been granted by comparison of the biometric data contained in the storage medium and provided by the user, the ability of a particular transaction to be finalised may depend on other parameters and not merely the authenticity of the user, including sufficient funds in a user's bank account to complete a transaction or general credit rating details in respect of the user.

In one preferred embodiment of the invention the sensor for access by the user to provide biometric data may be coupled by a hard wire system to a transaction switching network such as specialised phone lines such as those associated with the EFTPOS system. However, in other embodiments a wireless transmission system may be utilised and the sensor may be provided on a mobile transaction device such as that disclosed in our copending international patent application no. PCT/AU94/00247, the contents of which are incorporated into this specification by this reference. Thus, the device in our aforementioned international application may be modified to include a sensor for detecting a user's fingerprint and that data may be transmitted over a wireless transmission system with the information on the storage medium for comparison, may be compared in the device or may be compared in the card, and an access signal generated for transmission over the wireless transmission system to a host computer so that the financial transaction may continue or the data in the storage medium and that provided by the user may be transmitted to the host computer or the matching process could resident in the reading device for comparison in the host computer so that the host computer can generate the access signal to continue the transaction in the event of a match.

Preferably the support member includes a plurality of separate storage locations for storing data parcels, each data parcel being accessible separately upon receipt of an authorisation code so that only data contained in one or more data parcel, which relates to the authorisation code, is accessible.

This embodiment of the invention enables data parcels which relate to the individual who owns the card to be stored on the card such as vehicle licence details, credit card details, EFTPOS banking details, medical data, passport data and the like and to be accessible only when an appropriate authorisation code is presented to the card. Thus, at an airport, where only passport data is required, a card reader with which the card is used will present an authorisation code which will gain access only to the storage location containing the passport data so that only passport data can be read from the card and no other data contained in the card can be read. Similarly, other readers would be able to present authorisation codes which will gain access to other data parcels so that only data in that or those packages can be read by that reader. Thus, a single card can be used which contains a number of data parcels to allow a user to use a single card for credit card/EFTPOS transactions, as a driver's licence, passport or the like.

Preferably the plurality of separate storage locations are included in the circuit means.

Preferably each storage location is accessible by corresponding separate control programs stored in the circuit means so that when the storage medium is used with a reader, the reader supplies the authorisation code to the circuit means to cause one or more of the programs

corresponding to that authorisation code to access data in the data parcel stored in the storage location or locations which said one or more programs is able to access.

Preferably, the circuit means is in the form of a chip and the chip architecture is designed in such a way as to ensure that each program has access only to the memory location corresponding to that program where data relating to that program is to be held. This compartmentalising of the memory is to be controlled by the circuit means architecture and should ensure that it is impossible for the software to get around this feature so that one program can access memory in a storage location which does not correspond to that program.

Preferably communication between the storage medium and a reader is by a secure channel is created by a public key cryptograph system such as RSA. This system ensures secure communication between the card and the reader by the exchange of public keys from a randomly generated key set occurring between the storage medium and the reader for each and every communications session. The public keys are used to encrypt all subsequent communicated data between the card and the reader. The reader which receives the encrypted communication data must use the private key of its key set to gain access to the data. In this fashion, a secure communications layer is established between the storage medium and the reader rendering all transmitted data unintelligible to a third party observer.

Once the secured communication layer has been established, the reader must present the identification medium with a digital certificate as proof of its entitlement to communicate with the storage medium. This should occur before transfer of any data commences. In some

embodiments, a message authentication code may also be used to validate the data throughout the duration of the communications session between the storage medium and the reader.

The digital certificate may be included in the authentication code which activates the program for accessing data in the data parcels or may be a separate code to the authorisation code which activates the programs for accessing data.

A further aspect of the invention may be said to reside in an identification storage medium for storing data relating to a user, including:

a support member;

circuit means supported by the support member;

a plurality of separate data parcel storage locations in the circuit means for storing separate data parcels;

the circuit means also being for containing a plurality of access programs corresponding to the plurality of separate storage locations each for accessing data only in one of the storage locations corresponding to one of the programs; and

wherein, in use, when an authorisation code is received by the storage medium, one or more of the programs relating to that authorisation code is/are activated to cause the program to access data in one or more of the data parcels stored in the corresponding storage location or locations.

Preferably the circuit means is also for storing biometric data relating to the user of the medium.

This aspect of the invention may also be said to reside in

an identification system for providing access to an authorised user, including:

a storage medium having a support member circuit means supported by the support member, a plurality of separate data parcel storage locations in the circuit means for storing separate data parcels, the circuit means also being for containing a plurality of access programs corresponding to the plurality of separate storage locations each for accessing data only in one of the storage locations corresponding to one of the programs and wherein, in use, when an authorisation code is received by the storage medium, one or more of the programs relating to that authorisation code is/are activated to cause the program to access data in one or more of the data parcels stored in the corresponding storage location or locations; and

a reader for receiving the storage medium and supplying an authentication code to the card, the authentication code including a certificate which establishes the entitlement of the reader to communicate with the storage medium and an authorisation code for activating one or more of the programs.

Preferably the circuit means also stores biometric data relating to an authorised user of the storage medium and the reader includes an input means for receiving biometric data from the user and for comparing the biometric data stored on the storage medium with the biometric data provided by the user to establish the entitlement of the user to use the storage medium.

The invention may also be said to reside in an identification method for providing access to an authorised user, including storing data relating to the user in the form of a plurality of separate data parcels:

supplying an authorisation code to the storage locates so that the authorisation code causes only data in those storage locations which correspond to the authorisation code to be accessed.

Preferably the method also includes the step of storing biometric data relating to the authorised user of the storage medium and comparing the biometric data stored on the storage medium with biometric data provided by a user to establish the user's entitlement to use the storage medium.

The invention in a further aspect may be said to reside in a mobile funds transaction device for transferring funds between one facility and another facility, including:

an input unit having:

a card reader for reading data in or on a requester's card;

an input pad for the input of data relating to a transaction; and

an output report device for providing details of the transaction;

coupling means for electronically coupling the input unit to a wireless communication device;

a sensor for receiving biometric data from a user and producing an output signal indicative of the biometric data; and

wherein the input device, in use, provides an information signal including data relating to the transaction and data relating to the operator of the transaction device so that the coupling means can transfer the information signal to the wireless communication device so that the wireless communication device can, in turn, transmit the signal to a central facility to cause funds to be transferred from said one facility relating to the

requester to said another facility relating to the operator, and wherein the funds transaction device is mobile and portable and therefore can be moved from one location to another in view of the coupling means which couples the input unit to the wireless communication device to thereby enable the funds transaction device to be used without the need to be hard wired into a transmission system.

Preferably the device includes a processor means for comparing the biometric data provided by the user with biometric data stored in the card and for providing a signal upon match to enable the transaction to proceed. In other embodiments the biometric data stored in the card and that output signal indicative of the biometric data produced by the sensor may be transmitted to the central facility for comparison and production of an access signal.

Preferably the processor also controls the card reader, the input pad, the output report device and the coupling means.

The invention in a further aspect may also be said to reside in a funds transaction device for transferring funds between one card and another, including:

first input means for receiving a first card;

second input means for receiving a second card;

a sensor for receiving biometric data from at least one user and producing an output signal indicative of the biometric data; and

processing means for comparing the biometric data received by the sensor with biometric data included in at least one of the cards and for transferring funds from one of the cards to the other of the cards.

A preferred embodiment of the invention will be described,

by way of example, with reference to the accompanying drawings in which:

Figure 1 is a view of a card embodying the invention;

Figure 2 is a view of a device used in the preferred embodiment; and

Figure 3 is a diagram of a system according to the invention; and

Figure 4 is a diagram of a second embodiment of the invention.

With reference to figure 1 a card 10 is shown which include an integrated circuit 12. The card 10 may be any type of credit or identification card such as a stored value card, smart card, access card, id card, relationship card, medical card, merchant card, loyalty card, proprietary card or transport card etc.

The integrated circuit 12 forms a smart card chip which may include usual data relating to point of sale functions such as bank account details and the like. However, according to the preferred embodiment of the invention the chip which forms the integrated circuit 12 also include a digitised fingerprint of the authorised user so as to give it a high degree of portability and also enhanced security features.

The card 10 is intended to be used with a point of sale or access device 20 shown in figure 2. However, the card 10 could also be used with a device for card to card transfer of funds so that a credit balance in one person's card is transferred to another person's card without going through a banking facility or host computer. The device 20 includes a card reader 22 which may be slot into which the card 10 is inserted for reading data in the integrated circuit 12. The device 20 also has a key pad 24, a display

26, a printer 28 and a biometric scanner 30. Thus, the user's fingerprint is digitally recorded in the integrated circuit 12 on the card 10 and is read from the integrated circuit 12 by the card reader 22. The user then places his or her finger on the bio-recognition scanner 30 so that a digital template of the user's finger can be obtained and that template is compared with that stored in integrated circuit 12 on the card 10 by a processor 32. If a match is determined an access signal is produced by the processor 32. Alternatively, the comparison may take place in the circuit 12 on the card 10 rather than in the device 20 and if a match is established, data on the card can then be accessed or transferred.

The bio-recognition scanner 30 may also include additional security features to ensure that it is actually the authorised user's thumbprint which is being placed on the scanner and not some representation. This is done by looking at blood flow characteristics and determining changes in colour intensity when a person's finger is placed on the scanner to ensure that the actual finger is on the scanner and not a representation of the authorised user's finger.

As shown in figure 3, the device 20 transmits an access signal A to a host computer 50 associated with a bank or other facility so that a transaction can proceed. The keypad 24 may be accessed by the user or a vendor to insert details relating to a transaction such as the price of a product or amount of cash required and that data together with the access signal is transmitted to the host computer 50 for further processing so that the transaction can be authorised by the host computer 50 and an appropriate authorisation signal be transmitted back to the device 20 so that a receipt can be produced by the printer 28 or so

that cash can be dispensed from a dispenser (not shown).

The transmission of the signals A and B in figure 3 may be by hard wire over the conventional EFTPOS telephone system or may be a wireless transmission over the mobile telephone cellular network or via radio packet modem or the like. The device 20 may be a mobile transaction device similar to that disclosed in our abovementioned international application which provides wireless transmission of data and therefore is portable and can be used in the field without the need to be hard wired. The addition to the device of our international application is the bio-recognition scanner 30 which provides the digitised fingerprint of the user's finger for matching with the data concerning the finger template in the integrated circuit 12 of the card 10. In other embodiments, the bio-recognition scanner 30 may be separate from the device 20 and electronically linked to the device.

The device 20 therefore is for use with the card 20 which may be a smart card and includes the pin pad 24, a modem 41 which is coupled to the processor 32, a communication interface device 43 connected to the modem 41 with the processor 32 controlling the operation of the pin pad 24, the display 26, the printer 28 and the scanner 30 and also controlling operation of the wireless communication device 51, the modem 43 and the interface 41 to produce the wireless transmission of data to the host computer 50. The wireless communication device 51 may be a connection for connecting to a mobile telephone (not shown) so the mobile telephone network can be used for the transmission of data to the host computer 50 or the modem device 41, communication interface 43 and connection 51 may be replaced by a radio packet modem or the like (not shown) for wireless communication.

In the preferred embodiment of the invention the authorisation could also include a personal identification number which the user must key into the keypad 24 so that conventional personal identification number authorisation may be obtained in the event that the card is used with a point of sale device or automatic teller which does not have fingerprint scan facilities. As old machines are replaced with new machines which include facilities that comparison of the stored finger scan image and the image read by the terminal from the user's fingerprint the need to use a personal identification number can be eliminated.

Furthermore, a single card could be used instead of numerous cards since the integrated circuit 12 could be encrypted with not only the fingerprint template of the user but also bank account details for a number of financial institutions and also possibly with a credit amount for direct cash dealings from the card without access to the financial institution. Thus, the card according to the preferred embodiment of this invention can be regarded as an electronic wallet in which you would have cash (the stored cash value in the integrated circuit 12) and various credit, debit and charge account details also stored in the integrated circuit 12 along with the fingerprint template. Normally when purchasing something the user can choose a method of payment by either the cash stored value or the credit/debit or charge facilities.

Figure 4 shows a further embodiment of the invention.

In this embodiment of the invention the card 10 carries an integrated circuit 12 as per the previous embodiment. The integrated circuit 12 may include biometric data relating to the user of the card as previously described with reference to Figures 1 to 3 and which is accessed and

compared in the same way as in the embodiment of Figures 1 to 3.

In this embodiment of the invention, the integrated circuit 12 includes a plurality of separate storage locations D1 to Dn for storing separate data parcels which contain data relating to the user. Each of the separate data parcels may include data relating to:

credit card information;
EFTPOS banking information;
vehicle licence information;
passport information, medical data;
social welfare or security data.

The above mentioned kinds of data are listed merely by way of example and are not intended to be complete or exhaustive.

In this embodiment of the invention, a card reader 70 is intended to read data from only one or some of the data parcels mentioned above. For example, if the card reader 70 is located at an airport for processing passport applications, the reader 70 would only access the data parcel relating to the passport information. If the reader is in a hospital or the like, the reader may access only the medical data. If a credit card transaction is taking place, the reader 70 would access only the data relating to the relevant credit provider which is being used by the user or if an EFTPOS transaction is taking place, only the EFTPOS data.

In some embodiments, it may be desirable for a single reader 70 to access several of the data packages. For example, police or security organisations may access all of the data on the card from a single reader 70 and other

organisations or bodies may require data from several of the data parcels and therefore the reader 70 may access several of the data parcels.

The integrated circuit 12 is shown schematically on the left hand side of Figure 4 and includes interface or front end 25 and the plurality of separate storage locations D1 to Dn for storing the data parcels. Each of the storage locations D1 to Dn has a corresponding program P1 to Pn stored in the integrated circuit 12 which can access only the corresponding storage location. For example, program P1 accesses only storage location D1 and program Pn accesses only storage location Dn. Thus, n independent secure parcels of information are contained with the integrated circuit 12 at any one time. The different parcels of data included in the storage locations D1 to Dn require different access codes to be presented and validated before encrypted data parcels are supplied from the storage locates D1 to Dn to the card reader 70. Each storage location D1 to Dn not only requires a different access code but may also involve an entirely different encryption key for the securing of the data in that location and also possibly a different encryption algorithm could be used in the application of that key.

The different access codes may be interpreted from the biometric data stored in the circuit 12.

Each data parcel in the storage locations D1 to Dn is therefore only accessible through an independent program P1 to Pn which resides in the circuit 12. Each program P1 to Pn has access only to its own storage location D1 to Dn and is unable to retrieve information from any other storage location. The architecture of the circuit 12 is designed in such as way to ensure that each program P1 to Pn has

access only to its own memory location D1 to Dn where its own data parcel is to be held. This compartmentalising of the memory is controlled by the architecture of the circuit 12 so that it cannot be got around to ensure the security and integrity of the different data parcels. However, even if a program could access the contents of a data parcel not intended for use by it, it would not be possible for that program to use the information in any way due to the nature of its separate encryption.

Communication between the reader 70 and the card 10 is via a secure communication channel 90 shown schematically in Figure 4. When the card is used with the reader 70, the card 10 is located in a slot 74 and the user locates his or her thumb on scanner 72 so that the biometric data received by the scanner 72 can be compared with the data stored on the card 10 to establish the user's authenticity. The comparison most preferably takes place within the circuit 12 on the card 10 by the reader 70 transmitting data from the scanner 72 to the circuit 12. However, in other embodiments, the comparison could take place in the reader 70. The indication over the channel 90 is preferably under a public key cryptograph system with the exchange of public keys from a randomly generated key set occurring between the card 10 and the reader 70 for each and every communication session. These public keys will then be used to encrypt all subsequent communicated data between the card 10 and the reader 70 or its applications. The reader 70 which receives the encrypted communication must use the private key of its key-set to gain access to the data. In this fashion, a secure communication layer is established between the card 10 and the reader 74 rendering all transmitted data unintelligible to a third observer.

In the preferred embodiment of the invention, the

architecture of the chip 12 prevents lucid examination of the contents of the memory locations D1 to Dn, program execution and encryption function. Any evasive attack upon the security of the card preferably causes the erasure of all sensitive information.

Thus, the secure channel 90 is established by the card 10 generating random key-sets each having a private key which is basically a code retained within the card 12 and a public key which is corresponding to that private key an which is passed with data to the reader 70. The reader 70 also sends data back with the public key and uses its own private key to decrypt the data supplied with the public key supplied by the card 10. Similarly, data supplied back from the reader 70 with its public key is decrypted by the private key in the card 10.

The above mentioned form of public key encryption is known and therefore will not be described in further detail hereinafter.

Before any data is transmitted from the card 12 to the reader 70, the reader 70 must present a digital certificate which is a code which proves the authenticity of the reader 70 to the card before any data is transmitted. The digital certificate may include or comprise the authorisation code which activates one of the programs P1 to Pn to access the data parcel contained in the storage locations D1 to Dn or once the digital certificate is received and verified by the card 12, the authorisation code may be a separate code which is then supplied by the reader 70 for accessing one or more of the data parcels in the storage locations D1 to Dn.

Since modifications within the spirit and scope of the

invention may readily be effected by persons skilled within the art, it is to be understood that this invention is not limited to the particular embodiments described by way of example hereinabove.

THE CLAIMS DEFINING THE INVENTION ARE AS FOLLOWS:

1. An identification storage medium, including:

a support member; and

circuit means supported by the support member for storing biometric data relating to an authorised user of the medium.

2. The medium of claim 1, wherein the biometric data is a fingerprint template of the user.

3. The medium of claim 1, wherein the circuit means comprises an integrated circuit chip supported by the body of the credit card.

4. An identification system for providing access to an authorised user, including:

a storage medium having a support member, and

circuit means supported by the support member for storing biometric data relating to the authorised user;

a sensor for access by a user to provide biometric data to the system; and

processing means for comparing the biometric data stored in the circuit means with that detected by the sensor and for providing an access signal in the case of a match to thereby grant access to the authorised user.

5. An identification method for providing access to an authorised user, including:

storing biometric data relating to an authorised user on a storage medium;

comparing the biometric data stored on the storage medium with biometric data provided by a user; and

granting access to the authorised user in the case of a match between the data stored on the storage

medium and that provided by the user.

6. The medium of claim 1, wherein the support member includes a plurality of separate storage locations for storing data parcels, each data parcel being accessible separately upon receipt of an authorisation code so that only data contained in one or more data parcel, which relates to the authorisation code is accessible.

7. The medium of claim 6, wherein the plurality of separate storage locations are included in the circuit means.

8. The medium of claim 6, wherein each storage location is accessible by corresponding separate control programs stored in the circuit means so that when the storage medium is used with a reader, the reader supplies the authorisation code to the circuit means to cause one or more of the programs corresponding to that authorisation code to access data in the data parcel stored in the storage location or locations which said one or more programs is able to access.

9. The medium of claim 6, wherein the circuit means is in the form of a chip and the chip architecture is designed in such a way as to ensure that each program has access only to the memory location corresponding to that program where data relating to that program is to be held. This compartmentalising of the memory is to be controlled by the secure-microcontrollers hardware architecture and should ensure that it is impossible for the software to get around this feature so that one program can access memory in a storage location which does not correspond to that program.

10. An identification storage medium for storing data relating to a user, including:

a support member;

circuit means supported by the support member;

a plurality of separate data parcel storage locations in the circuit means for storing separate data parcels;

the circuit means also being for containing a plurality of access programs corresponding to the plurality of separate storage locations each for accessing data only in one of the storage locations corresponding to one of the programs; and

wherein, in use, when an authorisation code is received by the storage medium, one or more of the programs relating to that authorisation code is/are activated to cause the program to access data in one or more of the data parcels stored in the corresponding storage location or locations.

11. The medium of claim 10, wherein the circuit means is also for storing biometric data relating to the user of the medium.

12. An identification system for providing access to an authorised user, including:

a storage medium having a support member circuit means supported by the support member, a plurality of separate data parcel storage locations in the circuit means for storing separate data parcels, the circuit means also being for containing a plurality of access programs corresponding to the plurality of separate storage locations each for accessing data only in one of the storage locations corresponding to one of the programs and wherein, in use, when an authorisation code is received by the storage medium, one or more of the programs relating to

that authorisation code is/are activated to cause the program to access data in one or more of the data parcels stored in the corresponding storage location or locations; and

a reader for receiving the storage medium and supplying an authentication code to the card, the authentication code including a certificate which establishes the entitlement of the reader to communicate with the storage medium and an authorisation code for activating one or more of the programs.

13. The system of claim 12, wherein the circuit means also stores biometric data relating to an authorised user of the storage medium and the reader includes an input means for receiving biometric data from the user and for comparing the biometric data stored on the storage medium with the biometric data provided by the user to establish the entitlement of the user to use the storage medium.

14. An identification method for providing access to an authorised user, including storing data relating to the user in the form of a plurality of separate data parcels:

supplying an authorisation code to the storage locates so that the authorisation code causes only data in those storage locations which correspond to the authorisation code to be accessed.

15. The method of claim 14, wherein the method also includes the step of storing biometric data relating to the authorised user of the storage medium and comparing the biometric data stored on the storage medium with biometric data provided by a user to establish the user's entitlement to use the storage medium.

16. A mobile funds transaction device for

transferring funds between one facility and another facility, including:

an input unit having:

a card reader for reading data in or on a requester's card;

an input pad for the input of data relating to a transaction; and

an output report device for providing details of the transaction;

coupling means for electronically coupling the input unit to a wireless communication device;

a sensor for receiving biometric data from a user and producing an output signal indicative of the biometric data; and

wherein the input device, in use, provides an information signal including data relating to the transaction and data relating to the operator of the transaction device so that the coupling means can transfer the information signal to the wireless communication device so that the wireless communication device can, in turn, transmit the signal to a central facility to cause funds to be transferred from said one facility relating to the requester to said another facility relating to the operator, and wherein the funds transaction device is mobile and portable and therefore can be moved from one location to another in view of the coupling means which couples the input unit to the wireless communication device to thereby enable the funds transaction device to be used without the need to be hard wired into a transmission system.

17. The device of claim 16, wherein the device includes a processor means for comparing the biometric data provided by the user with biometric data stored in the card and for providing a signal upon match to enable the

transaction to proceed. In other embodiments the biometric data stored in the card and that output signal indicative of the biometric data produced by the sensor may be transmitted to the central facility for comparison and production of an access signal.

18. The device of claim 17, wherein the processor also controls the card reader, the input pad, the output report device and the coupling means.

19. A funds transaction device for transferring funds between one card and another, including:

first input means for receiving a first card;

second input means for receiving a second card;

a sensor for receiving biometric data from at least one user and producing an output signal indicative of the biometric data; and

processing means for comparing the biometric data received by the sensor with biometric data included in at least one of the cards and for transferring funds from one of the cards to the other of the cards.

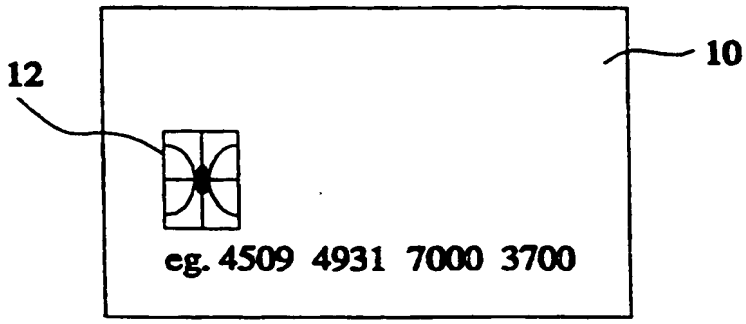


Figure 1.

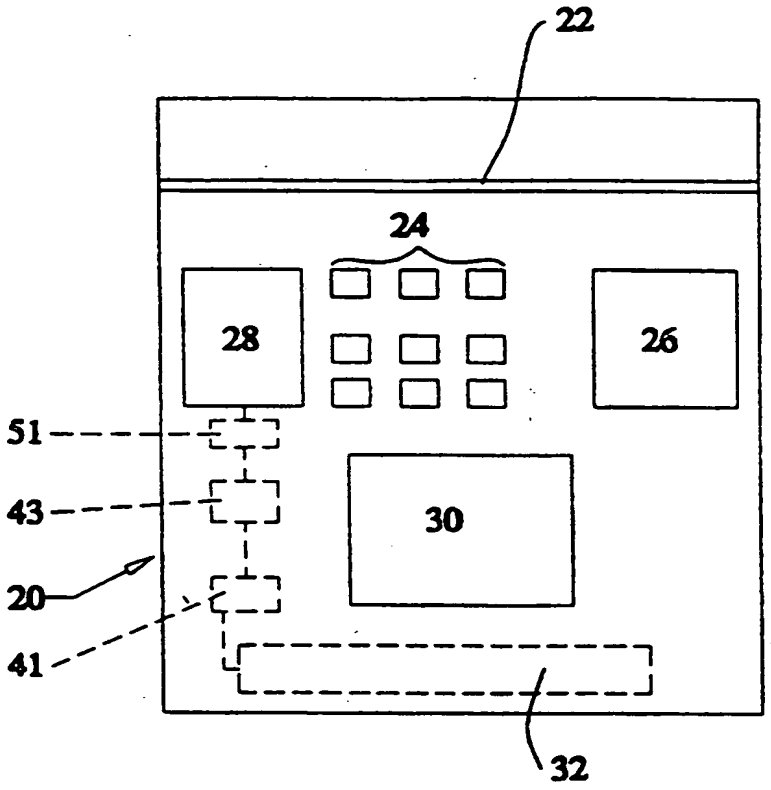


Figure 2.

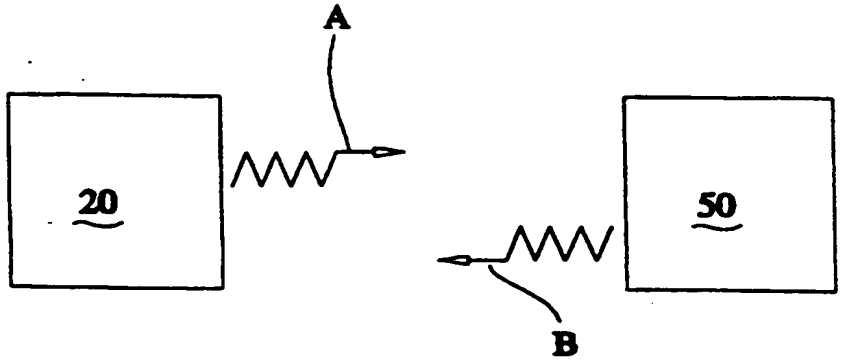


Figure 3.

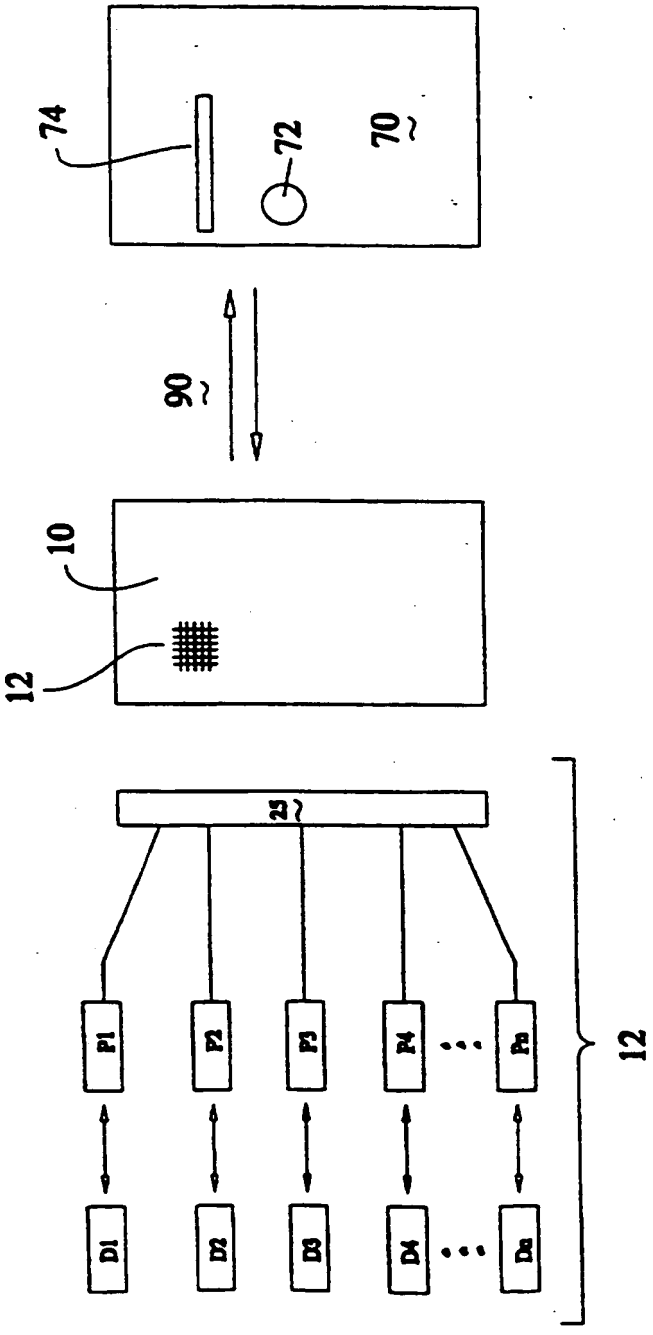


Figure 4.

INTERNATIONAL SEARCH REPORT

International Application No. PCT/AU 97/00426

A. CLASSIFICATION OF SUBJECT MATTER

Int Cl[6]: G06K 19/073, B42D 15/10 // 109:00, //201:00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC:G06K 19/073, B42D 15/10//109:00, //201:00, G06F 17/60 //157:00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
AU IPC as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
INSPEC Keywords[(biometric, fingerprint, iris, DNA, biological) and (wireless, radio, rf) and ((card:) and (circuit: or smart))]

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y	FINANCIAL TECHNOLOGY INSIGHT, REES. F. "Intags smartcard set to incorporate biometrics" (August 1994), page 5 See entire document	1-9 10 to 18
X	FR 2694421 A (BERTIN & CIE), 4 February 1992 Se whole document	1, 2, 6-9
X	The Stephen Cobb Complete Book of PC and LAN Security, STEPHEN COBB, 1992, page 194 to 201 See whole document	1,2,4 to 12, 15

[X] Further documents are listed in the continuation of Box C

[X] See patent family annex

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search
25 August 1997

Date of mailing of the international search report
01 SEP 1997

Name and mailing address of the ISA/AU
AUSTRALIAN INDUSTRIAL PROPERTY ORGANISATION
PO BOX 200
WODEN ACT 2606
AUSTRALIA Facsimile No.: (02) 6285 3929

Authorized officer
ROBERT BARTRAM
Telephone No.: (02) 6283 2215

INTERNATIONAL SEARCH REPORT

International Application No.
PCT/AU 97/00426

C (Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 91/06920 (TMS INCORPORATED), 31 October 1990, G06K 9/00, Claims 3, 32, and 55 are particularly relevant.	1 to 18
X	WO 89/12287 (TRIPEAU), 14 December 1989 See whole document	1 to 18
X	FR 2634570 (REITTER et al) 26 January 1990 See whole document	1 to 18
X	DE 3706466 (SIEMENS AG) 8 September 1988 See whole document	1 to 18
Y	AU 669321 (DYNAMIC DATA SYSTEMS PTY LTD) 30 May 1996 See whole document	10 to 18
Y	AU 669322 (DYNAMIC DATA SYSTEMS PTY LTD)30 May 1996 See whole document	10 to 18
Y	US 5408513 (BRUSCH. Jr. et al), 18 April 1995 See whole document	16 to 18
Y	US 5294782 (KUMAR), 15 March 1994 See whole document	1 to 18
Y	WO 83/03694 (BENTON), 27 October 1983 See whole document	16 to 19

INTERNATIONAL SEARCH REPORT
Information on patent family members

International Application No.
PCT/AU 97/00426

This Annex lists the known "A" publication level patent family members relating to the patent documents cited in the above-mentioned international search report. The Australian Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

Patent Document Cited in Search Report		Patent Family Member					
FR	2694421						
WO	9106920	AU	67230/90	US	5363453	AU	37497/89
		FR	2632102	WO	8912287		
FR	2634570						
DE	3706466						
US	5408513						
US	5294782	AU	27564/92	EP	605630	JP	7501903
		US	5294782	WO	9306564	US	5386106
		US	5489773				
WO	8303694	BR	8300478	EP	112814	US	4454414
AU	47934						
AU	47933						

END OF ANNEX

INTERNATIONAL SEARCH REPORT

International Application No.
PCT/AU 97/00426

Box 1 Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)

This International Search Report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☒ Claims Nos.: 14
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:
the identification method defined is very broad in scope and specific classification of this claim is not possible.

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a)

Box II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

Claims 1 to 9, 11, 13 and 15 to 18 define the use of biometric data to allow access to data on a storage medium, however claims 10, and 12 use authorisation code access. This is considered as very different access method and is therefore lacking in unity of invention.
In addition claim 14 is considered as not conforming to a unity of invention. Claim 19 introduces the aspect of a second card for transferring of data to and from. This is considered as requiring substantially different features and is therefore considered as lacking in unity.

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims

2. ☒ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest.

☐ No protest accompanied the payment of additional search fees.